UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,516	05/23/2000	Xin Qiu	018926-002110US	4301

7590 04/26/2006

Motorola, Inc.
Robert P. Marley
Broadband Communications Sector
101 Tournament Drive
Horsham, PA 19044

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/576,516	QIU ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26 and 28-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26 and 28-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20040322*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 and 28-32.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/04/2006 has been entered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 21-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the

claimed invention. Claim 21 recites, "said Decreased Security Authorization Code is separate from said Decreased Security Authorization Code" nowhere in the specification is there a description of how to make a code be separate from itself.

5. Claims 21-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 21 recites, "said Decreased Security Authorization Code is separate from said Decreased Security Authorization Code" it is impossible for a code to be separate from itself and one of ordinary skill in the art would not know how to make a code separate from itself.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-26 and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grube et al (US 5602916) in view of Hayashi et al (US 5930361).

As per claim 1, Grube et al discloses a method of providing varying levels of security in a data processing system (see fig. 4, sheet 3, col. 2, lines 39-57), receiving information from an outside source (see col. 2, lines 58-67, col. 3, lines 1-20), retrieving an indicator from the received information that instructs the system to operate at a higher level of security (see col. 3, lines 39-62, col. 5, lines 25-38).

Grube et al fails to disclose the reception of a second indicator to proceed to a lower security level and preventing operation at the second level until the reception.

However, Hayashi et al teaches such a second indicator (see column 1 line 52 through column 2 line 7).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include Hayashi et al's second indicator in the system of Grube et al.

Motivation to do so would have been to allow a user to view a transmission that was previously unauthorized (see column 1 line 52 through column 2 line 7).

As per claim 2, the modified Grube et al and Hayashi et al system discloses receiving an encrypted message (see Grube et al col. 4, lines 7-20).

As per claim 3, the modified Grube et al and Hayashi et al system discloses wherein said Decreased-security Authorization-Code authorizes a decrease in encryption/decryption level (see Grube et al col. 3, lines 45-65).

As per claim 4, the modified Grube et al and Hayashi et al system discloses wherein said Decreased-security Authorization-Code authorizes a decrease in authentication level (see Grube et al col. 3, lines 45-65).

As per claim 5, the modified Grube et al and Hayashi et al system discloses wherein said Decreased-security Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels (see Grube et al col. 3, lines 45-65).

As per claim 6, the modified Grube et al and Hayashi et al system discloses wherein said encrypted message further comprises a key for use in a decryption algorithm (see Grube et al col. 4, lines 7-45).

As per claim 7, the modified Grube et al and Hayashi et al system stores a master key (i.e. unique user key) to decrypt messages includes new decryption key values and using said

master key stored at said system to decrypt said encrypted message (see Grube et al col. 3, lines 59-67, col. 4, lines 1-45).

As per claim 8, the modified Grube et al and Hayashi et al system discloses establishing a Security-Level-status-Indicator at said system to indicate a level of security that is being implemented (see Grube et al fig. 3, sheet 2).

As per claim 9, the modified Grube et al and Hayashi et al system discloses said Security-Level-status Indicator indicates a level of encryption/decryption that is being implemented by the system (see Grube et al fig. 3, sheet 2, col. 3, lines 59-65, col. 5, lines 26-44).

As per claim 10, the modified Grube et al and Hayashi et al system discloses said Security-Level-status Indicator indicates a level of authentication that is being implemented by the system (see Grube et al col. 3, lines 59-67).

As per claim 11, the modified Grube et al and Hayashi et al system discloses said Security-Level-status Indicator indicates a level of authentication and a level of encryption/decryption that is being implemented by the system (see Grube et al col. 3, lines 45-65).

As per claim 12, the modified Grube et al and Hayashi et al system discloses configuring said Security Level Status

Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels (see Hayashi et al column 1 line 52 through column 2 line 7).

As per claim 13, the modified Grube et al and Hayashi et al system discloses utilizing a cable head-end as said outside source including a set-top box (see Hayashi et al column 1 line 52 through column 2 line 7).

As per claim 14, the modified Grube et al and Hayashi et al system discloses using a Key Management Message to convey said Decreased Security Authorization Code (see Grube et al col. 3, lines 45-65).

As per claim 15, the modified Grube et al and Hayashi et al system discloses wherein delivery of said Key Management Message is authenticated (see Grube et al col. 36-47).

As per claim 16, the modified Grube et al and Hayashi et al system discloses wherein delivery of said Key Management Message is protected against a replay attack (see Grube et al col. 7, lines 35-65).

As per claim 17, the modified Grube et al and Hayashi et al system discloses wherein delivery of said Key Management Message is authenticated and protected against a replay attack (see Grube et al col. 8, lines 1-30).

As per claim 18, the modified Grube et al and Hayashi et al system discloses wherein a lower level of security is nonpublic Key mode, wherein a higher level of security is a public Key mo' de, continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source (see Grube et al col. 3, lines 53-65).

As per claim 19, rejected under the same basis as claim 7.

As per claim 20, recites limitations already rejected (see claim: 1 and 12).

As per claim 21, the modified Grube et al and Hayashi et al system discloses a cryptographic device an input to receive a data stream originated by a sending party; a Security -Level-status-Indicator; and code means for executing a cryptographic algorithm wherein said cryptographic algorithm is indicated by said Security-Level-status-Indicator (see Grube et al col. 3, lines 59-67, col. 5, lines 26-44, fig. 3, sheet 2), and a code means for decrypting a decreased security authorization code originated by the sending party (see Grube et al col. 7, lines 24-35).

As per claim 22, the modified Grube et al and Hayashi et al system discloses wherein said code means for executing a cryptographic algorithm comprises code means for executing a high level cryptographic algorithm and code means for executing

a low level cryptographic algorithm relative to said high level cryptographic algorithm (see Grube et al fig. 3, lines 59-67).

As per claim 23, the modified Grube et al and Hayashi et al system discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and wherein said low level cryptographic algorithm comprises a low level decryption algorithm (see Grube et al col. 3, lines 53-65).

As per claim 24, the modified Grube et al and Hayashi et al system discloses wherein said high level cryptographic algorithm comprises a high level authentication algorithm and wherein said low level cryptographic algorithm comprises a low level authentication algorithm (see Grube et al col. 7, lines 24-35).

As per claim 25, the modified Grube et al and Hayashi et al system discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and a high level authentication algorithm and wherein said low level cryptographic; algorithm comprises a low level decryption algorithm and a low level authentication algorithm (see Grube et al col. 3, lines 59-67, col. 7, lines 24-35).

As per claim 26, the modified Grube et al and Hayashi et al system discloses wherein said high level cryptographic algorithm is a public Key encryption algorithm and wherein said low level

cryptographic algorithm is a non-public Key encryption algorithm (see Grube et al col. 3, lines 53-65).

As per claim 28, the modified Grube et al and Hayashi et al system discloses and means for preventing a replay attack in delivery of said Decreased-security Authorization-code (see Grube et al col. 8, lines 1-30).

As per claim 29, the modified Grube et al and Hayashi et al system discloses a master key to use in decrypting said Decreased Security Authorization Code (see Grube et al col. 3, lines 59-67, col. 4, lines 1-45).

As per claim 30, the modified Grube et al and Hayashi et al system discloses wherein said Security Level Status Indicator is encrypted (see Grube et al col.7, lines 36-50).

As per claim 31, the modified Grube et al and Hayashi et al system discloses providing a receiver to receive a transmission (see Grube et al col. 2, lines 58-67, col. 3, lines 1-20); establishing a Security-Level-status-Indicator at said receiver (see col. 3, lines 59-67) establishing a first level of decryption at said receiver (see col. 3, lines 59-67, col. 4, lines 1-20); encrypting a first message at a first level of encryption (see col. 3, lines 59-67, col. 4, lines 1-20) transmitting said first message to said receiver at said first level of encryption (see col. 2, lines 58u67, col. 3, lines 1-

20); receiving said first message at said receiver (see col. 7, lines 36-65); decrypting said first message encrypted at said first level of encryption (see col. 7, lines 36-65); transmitting a Decreased-security-Authorization Code to change from said first level of decryption to a second level of decryption (see col. 3, lines 12-58); receiving said Decreased-security-Authorization-code; determining a change in encryption level from said first level of encryption to said second level of encryption (see fig. 3, lines 59-67, col. 4, lines 1-5) adjusting said Security-Level-status-Indicator at said receiver (see fig. 3, sheet 2); encrypting a second message at said second level of encryption (see col. 3, lines 59-67, col. 4,lines 1-5); transmitting said second message at said second level of encryption; receiving said second message at said receiver; and decrypting said second message at said receiver (see col. 4, lines 7-20, 49-67; see also Hayashi as applied to claim 1).

As per claim 32, it is rejected under the same basis as claim 31.

Response to Arguments

8. Applicant's arguments with respect to claims 1-26 and 28-32 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Laczko et al (US 6266754 B1), Handelman et al. (US 5878134 A), Formosa (US 6154525 A), Gammie (US 5029207 A), Bradley et al. (US 5172413 A), Callais et al. (US 3790700 A), Hirose (US 5917915 A), Rix et al. (US 6385317 B1) each teach methods of providing an end system with a message in order for the end system to enable pay TV.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER